Local encoding of classical information onto quantum states

Yu Tanaka[1], Damian Markham[1], Mio Murao[1,2]

[1] *Department of Physics, Graduate School of Science, University of Tokyo, Tokyo 113-0033 Japan*
[2] *PRESTO, JST, Kawaguchi, Saitama 332-0012, Japan*

In this article we investigate the possibility of encoding classical information onto multipartite quantum states in the distant laboratory framework. We show that for all states generated by Clifford operation there always exist such an encoding, this includes all stabilizer states such as cluster states and all graph states. We also show encoding for classes of symmetric states (which cannot be generated by Clifford operations). We generalise our approach using group theoretic methods introducing the unifying notion of *Pseudo Clifford* operations. All states generated by Pseudo Clifford operations are locally encodable (unifying all our examples), and we give a general method for generating sets of many such locally encodable states.

arXiv:quant-ph/0702190v1 20 Feb 2007

I. INTRODUCTION

In quantum information we are often operating in a framework of separate distant laboratories, and the questions of what is possible or impossible under these local restrictions is crucial for understanding how we can use quantum resources in the best way. Through these considerations we have come to see entanglement as a resource for example for quantum cryptography [1, 2], teleportation [3], dense coding [4] and measurement based quantum computing [5]. Beyond this however, when considering local access of information encoded onto quantum states, we have also seen non-local features without the presence of entanglement [6].

We now turn to consider the complement of this problem, that of local encoding of information. As well as being interesting in its own right as a local restricted task, and as a complement to local access of information (and associated notions of locality), the ability to locally encode information is in fact an important part of many quantum information protocols. Indeed the first stage of dense coding (in fact, the encoding part) is precisely local encoding of classical information. It is also strongly connected to the problem of local unitary equivalence which plays a large role in entanglement theory (as we will see below).

In this paper we raise the question “can we locally encode on all states?”. That is, given an arbitrary state, can we use this as a quantum resource and encode the maximum classical information possible. Although this is a simple question, the answer is surprisingly difficult to find, and we find that we cannot give a positive or negative answer, other than to give a large set of examples where we can encode, and show how to encode and we are unable to find any example that we cannot locally encode.

Since classical information is completely distinguishable, the problem of encoding classical information on a state, becomes the problem of generating an orthogonal bases from that state. Then, our question becomes ”is it possible to locally generate a complete basis from all states”. In this way local encoding is related to local unitary equivalence of states. Though we may naively expect this to be simple to answer, there are hints that it is a hard question, explaining why we have been unable to find the solution. The strongest such hint comes from the existence of unextendible product bases [7]. This is a set of orthogonal product states who’s compliment must be entangled - that is it is impossible to find another state orthogonal this set which is product. This is an example that if we do not choose appropriate encoding operators, full local encoding is not possible (even though there may exist another set of local operations to encode full classical information).

We begin in section II by considering the local encoding of general product states. Our approach is then to take this encoding and extend it to sets of entangled states generated by unitaries which obey certain commutation relations. We concentrate on using Pauli operations to encode the states, where we develop the notion of *Pseudo* Clifford operations whose properties allow us to give a general sufficient condition for the ability to locally encode on a state. In particular this gives a method for locally encoding all stabiliser states, including cluster states used in measurement based quantum computation [5], CSS error correction code states and all graph states [8]. In section III we show local encoding for sets of symmetric states as examples of non-Clifford but Pseudo Clifford states. In section IV we use group analysis to investigate what states can be locally encoded by the methods we have introduced. We note that although in our methods we are restrictive on the allowed encoding operations (i.e. Pauli and derived from the product state case), our approach manages to cover all the states we consider here, and we have no example of states which we can show cannot be encoded by our methods.

II. LOCAL ENCODING ON PSEUDO CLIFFORD STATES

The problem of local encoding of classical information is equivalent to that of generating a basis by local operations. We begin by giving a formal definition of local encoding:

Definition II.1 *A n-qubit quantum state $|\psi\rangle$ is said to be locally encodable if there exists a set $\{v_i \mid v_i \in SU(2)^{\otimes n}\}_{i=0}^{2^n-1}$ of local unitary operations such that $\langle\psi| v_i^\dagger v_j |\psi\rangle = \delta_{ij}$ for all i, j. We call such $\{v_i\}$ the local encoder set.*

By this definition, we can always ignore the global phase of the encoded state $v_i |\psi\rangle$, since we only require orthogonality between the encoded states.

The difficulty of finding the local encoder lies in that the condition $\langle\psi| v_i^\dagger v_j |\psi\rangle = \delta_{ij}, \forall i, j$ in Definition II.1 is a weak condition, it only restricts the property of a local encoder $\{v_i\}$ applied to the given state $|\psi\rangle$. Given a state $|\psi\rangle$ it is difficult to check if there exists an encoding set, since we must search over all possible local unitaries. In this sense it is too weak to be easily checkable.

It is not strong enough to efficiently search the appropriate local encoder. In this paper, we take another approach to understand the properties of local encoding; First we pose a restriction on the local encoder to be tensor products of the Pauli operations $\{I, X, Y, Z\}$ represented by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

in the computational basis $\{|0\rangle, |1\rangle\}$ and obtain sufficient conditions for locally encodable states. Then we consider gradually relaxing the restriction to find wider classes of states which can be locally encodable and constructions of the local encoders.

Our restriction of the local encoder to consist of the Pauli operations allows group theoretical analysis. A set of 4^n n-tensor products operations consisting of the Pauli operators $\{I, X, Y, Z\}$ together with their overall phase of ± 1 or $\pm i$ constructS a group, which is called the *Pauli group* denoted by $\mathcal{P}$ (here we say the Pauli group on n-qubits is given by the tensor products of all qubit Pauli operators). Including the phase factor, the number of elements of the n-qubit Pauli is $4 \cdot 4^n$. For local encoding, we ignore the global phase factor and only care about 4^n elements of Pauli group operators.

To investigate local encoding, we use the properties of the Pauli group and another group, the *Clifford group*, generated by the Pauli group operators. The Clifford group is a group consisting of operators which leave the $\mathcal{P}$ fixed conjugation, and denoted by $\mathcal{C}$. Formally, it is defined by a set of operator C described by $\{C \in SU(2^n) | CpC^\dagger \in \mathcal{P},\ \forall p \in \mathcal{P}\}$. The Clifford group is generated by Hadamard gate H, the Phase gate S and the control-NOT gate U_{CNOT} represented in the computational basis by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},\ U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2}$$

in addition to the Pauli operations.

We first consider encoding product states. If the given state is a simple product states such as a zero state, which is n-tensor products of zero states defined by $|\bar{0}\rangle \equiv |0\rangle^{\otimes n} = |0\rangle \otimes |0\rangle \otimes ... \otimes |0\rangle$, it is apparent that a local encoder set is given by $v_0 = I \otimes ... \otimes I \otimes I$, $v_1 = I \otimes ... I \otimes X$, $v_0 = I \otimes ... X \otimes X$, ... ,$v_{2^n-1} = X \otimes ... X \otimes X$. This construction is based on the fact that we can "flip" each single qubit state $|0\rangle$ to $|1\rangle$ by performing a Pauli operation X. The all combinations of $\{I, X\}$ for n-qubits acting on $|\bar{0}\rangle$ give a set of states, which is a complete orthonormal set of the states denoted by $\{|\bar{i}\rangle\}$. We denote the local encoder set of the zero state by $\{v_i^{\bar{0}}\}$ and it is written by

$$\{v_i^{\bar{0}} \equiv v_i = X^{m_1} \otimes ... \otimes X^{m_n}\} \tag{3}$$

where a set of numbers $\{m_1, m_2, ..., m_n\}$ is a binary representation of i.

We generalize this way of local encoding to any product state. A general n-qubit product state $|\phi_p\rangle$ is represented by n-tensor products of single qubit states $|\phi_k\rangle = \cos(\theta_k/2)|0\rangle + e^{i\varphi_k}\sin(\theta_k/2)|1\rangle$ where θ_k and φ_k are positive parameters for kth qubit satisfying $0 \le \theta \le \pi$ and $0 \le \phi \le 2\pi$. These parameters represent the angles of the state vector $|\phi_p\rangle$ on the Bloch sphere. We consider how to perform a flip operation using a *minimum* number of parameters for a general $|\phi_k\rangle$ to make it as simple and general as possible. It is known that there is no universal flip operation for arbitrary states [9]. If we use two real parameters θ_k and φ_k, we can always transform $|\phi_k\rangle$ back into $|\bar{0}\rangle$, so it is

$$\begin{tikzcd} |0\rangle \arrow[r, "U"] \arrow[d, "\{w_i\}"'] & |\psi\rangle \arrow[d, "\{v_i\}"] \\ \{|i\rangle\} \arrow[r, "V"] & \{|\psi_i\rangle\} \end{tikzcd}$$

FIG. 1: The relationship of operations v_i, w_i, U, and V for local encoding of $|\psi\rangle = U|\bar{0}\rangle$ by the local encoder $\{v_i\}$. The set $\{\omega_i\}$ encode $|0\rangle$ to basis $\{|i\rangle\}$, and the set $\{v_i\}$ locally encode $|\psi\rangle = U|\bar{0}\rangle$ to $\{|\psi_i\}$, in accordance with EQN (5).

trivial to find the flip operation. In fact, we can describe a flip operation with just a single real parameter, since a state in the form of $|\phi_X\rangle \equiv \cos(\theta_k/2)|0\rangle + i\sin(\theta_k/2)|1\rangle$ can be flipped by X operation irrespective to the parameter θ_k. In the Bloch sphere picture, the state $|\phi_X\rangle$ is on the yz-plane, therefore the X operation (which proportional to a π-rotation around the x-axis) transforms $|\phi_X\rangle$ into its orthogonal state $\left|\phi_X^\perp\right\rangle$. Noting that a general single-qubit state $|\phi_k\rangle$ is transformed to $|\phi_X\rangle$ by a modified phase gate (a rotation around the z-axis until the state lies on the $z-y$plane)

$$s(\varphi_k) = \begin{pmatrix} 1 & 0 \\ 0 & ie^{-i\varphi_k} \end{pmatrix}, \tag{4}$$

the flip operation for each $|\phi_k\rangle$ is given by $X \cdot s(\varphi_k)$.A possible local encoder set of a general product state $|\phi_p\rangle$ is given by $\{v_i^{\bar{0}} \cdot s(\varphi_k)^{\otimes n}\}$ where $s(\varphi_k)^{\otimes n} = s(\varphi_1) \otimes ... s(\varphi_n)$ is independent of i.

Our strategy now is to try to use our knowledge about the local encoder of arbitrary product states for constructing the local encoders of entangled states. For this purpose, we introduce a representation of a n-qubit state $|\psi\rangle$ by using a (generally non-local) unitary operation U on the zero state $|\bar{0}\rangle$, namely, $|\psi\rangle = U|\bar{0}\rangle$. We note that by this relation, the unitary operation U is not uniquely determined, only the first column of U is determined.

Using the unitary representation, the conditions for local encoding is written by $\langle\bar{0}| U^\dagger v_i^\dagger v_j U |\bar{0}\rangle = \delta_{ij}$. We rewrite this relationship as

$$\langle\bar{0}| U^\dagger v_i^\dagger V V^\dagger v_j U |\bar{0}\rangle = \langle\bar{0}| w_i^\dagger w_j |\bar{0}\rangle = \delta_{ij} \tag{5}$$

where V is an arbitrary (non-local) unitary operation and $w_i \equiv V^\dagger v_i U$. We can view this relationship of v_i, w_i, U, and V in Figure 1.

Now we introduce a simplification. We consider a case that *both* $|v_i\rangle$ and $|w_i\rangle$ are given by n-tensor products of Pauli operations and also impose $V = U$. Then we can immediately see that if U is an operator belong to the Clifford group $\mathcal{C}$, which maps all tensor products of Pauli operators into another tensor products of Pauli operators, therefore, $w_i = U^\dagger v_j U$ is satisfied. We know from Eq.(3), the local encoder of the zero state $|\bar{0}\rangle$ is given by $\{w_i = v_i^{\bar{0}}\}$, therefore, all the Clifford group states represented by $|\psi\rangle = U|\bar{0}\rangle$ where $U \in \mathcal{C}$ is locally encodable by $\{v_i = U v_i^{\bar{0}} U^\dagger\}$.

We note that our condition of $U^\dagger v_j U = w_i$ should be only satisfied by 2^n elements of the local encoder $\{v_i\}$ out of 4^n different tensor products of the Pauli group operations. Thus, U can be taken to be in a larger class of operators than the Clifford group operators, which satisfy the condition $U^\dagger v_j U = w_i$ for all the elements of the Pauli group. We call the set of operators $\{U\}$ which satisfies $U^\dagger v_j U = w_i$ for 2^n different tensor products of the Pauli operators as the *Pseudo Clifford set* denoted by $\mathcal{PC}$ (a formal definition will be given in section IV). We will present constructions of local encoders for the states which are not generated by the Clifford group operations, but the Pseudo Clifford set operations from $|\bar{0}\rangle$ in section III. The group-like properties of the Pseudo Clifford set is investigated further in section IV. By definition, all Pseudo Clifford generated states can be locally encoded.

Now we consider how much we can extend the class of U beyond the Pseudo Clifford sets. Obviously, if a given entangled state $|\psi\rangle = U|\bar{0}\rangle$ is locally encodable by a local encoder set $\{v_i\}$, any locally equivalent state of the given state denoted by $|\psi\rangle_{LE} = u_1 \otimes ... \otimes u_n |\psi\rangle$ where $u_k \in SU(2)$ is locally encodable by $\{v_i \cdot u_1^\dagger \otimes ... \otimes u_n^\dagger\}$. This indicates the degree of freedom for the choice of the basis of the Pauli operations does not effects the ability of local encoding.

We further extend the class of U in the following way. A general product state $|\phi_p\rangle = \left(\cos(\theta_k/2)|0\rangle + e^{i\varphi_k}\sin(\theta_k/2)|1\rangle\right)^{\otimes n}$ is represented by $s(-\varphi_k)^{\otimes n} \cdot r(\theta_k)^{\otimes n}|\bar{0}\rangle$ where $r(\theta_k)$ is given by

$$r(\theta_k) = \begin{pmatrix} \cos(\theta_k/2) & -i\sin(\theta_k/2) \\ i\sin(\theta_k/2) & \cos(\theta_k/2) \end{pmatrix}, \tag{6}$$

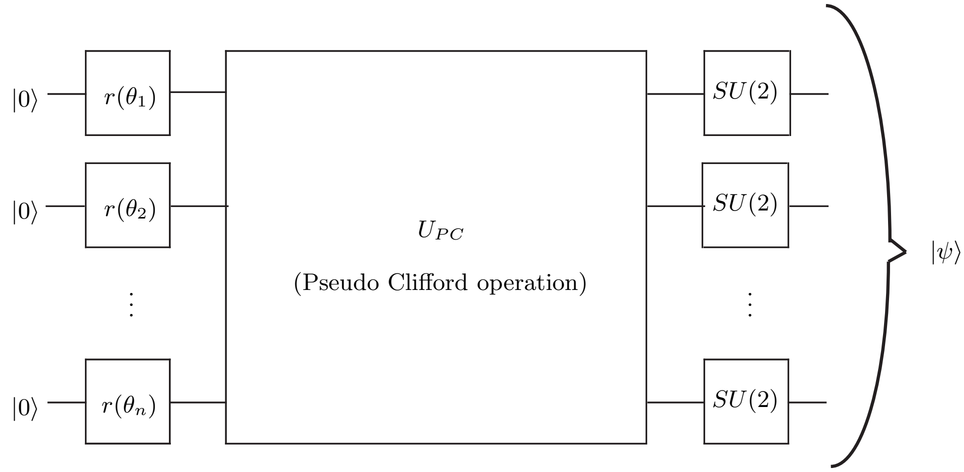

FIG. 2: All states $|\psi\rangle$ generated by the above circuit can be locally encoded (c.f. Theorem II.1). $r_{(\theta_k)}$ represents a θ_k rotation about x-axis for the kth qubit.

which is an operation proportional to a θ_k-rotation about x-axis. A state represented by $w_j |\bar{0}\rangle$ can be also represented by $w_j |\bar{0}\rangle = w_j \cdot r(-\theta_k)^{\otimes n} r(\varphi_k)^{\otimes n} |\phi_p\rangle$. Since we know that the general product state $|\psi_P\rangle$ is locally encodable by $\{v_i^{\bar{0}} \cdot s(-\varphi_k)^{\otimes n}\}$, we have $w_j = v_i^{\bar{0}} \cdot r(\theta_k)^{\otimes n}$. The local encoding condition for entangled states U is now given by

$$\langle\bar{0}| U^\dagger v_i^\dagger v_j U |\bar{0}\rangle = \langle\bar{0}| r(-\theta_k)^{\otimes n} (v_i^{\bar{0}})^\dagger v_j^{\bar{0}} \cdot r(\theta_k)^{\otimes n} |\bar{0}\rangle = \delta_{ij}. \tag{7}$$

Therefore, if the states represented by a Pseudo Clifford operation U, the states represented by $U \cdot r(\theta_k)^{\otimes n}$ are also locally encodable, and the local encoder is the same as the states represented by U.

To summarize the results obtained in this section, we have the following theorem:

Theorem II.1 ***Decomposition condition***
A n-qubit state $|\psi\rangle$ represented by $|\psi\rangle = U' |\bar{0}\rangle$ is locally encodable if U' can be decomposed into the form of $U' = (u_k)^{\otimes n} \cdot U \cdot s(\theta_k)^{\otimes n}$ where $u_k \in SU(2)$, U is given by a unitary operator in the Pseudo Clifford set $\mathcal{PC}$, and $r(\theta_k)$ is an arbitrary single qubit rotation about the x-axis. The local encoder is then given by

$$\{v_i = U_{PC} \cdot v_i^{\bar{0}} \cdot U_{PC}^\dagger \cdot ((u_k)^\dagger)^{\otimes n}\}. \tag{8}$$

As an example of this result, we show that any two qubit state is locally encodable. Two qubit states can be represented by the Schmidt decomposition form as $|\psi\rangle = \cos(\theta/2) |a_0\rangle \otimes |b_0\rangle + \sin(\theta/2) |a_1\rangle \otimes |b_1\rangle$. The Schmidt decomposition state can be represented by

$$u_1 \otimes u_2 \cdot U_{CNOT} \cdot (s(\pi) \cdot r(\theta)) \otimes I |\bar{0}\rangle, \tag{9}$$

where u_1 and u_2 map a computational basis $\{|i\rangle\}$ into $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$, respectively (See Fig. 3. Note that $s(\pi) = S \cdot Z$ therefore it is a Clifford operation, thus, this state is always locally encodable by $\{v_i = (s(\pi) \otimes I) \cdot U_{CNOT} \cdot v_i^{\bar{0}} \cdot U_{CNOT} \cdot (s(\pi) \otimes I) \cdot u_1^\dagger \otimes u_2^\dagger\}$.

Further, theorem II.1 also means that all stabiliser states can be locally encoded. This includes cluster states used in measurement based quantum computation [5], CSS error correction code states and all graph states [8].

III. LOCAL ENCODING ON SYMMETRIC BASIS STATES (A LARGE CLASS OF EXAMPLES)

We now focus on the Pseudo Clifford operation part and investigate local encoders for the states generated by the non-Clifford but Pseudo Clifford operations $U \in \mathcal{PC}$ by imposing an additional condition $w_i = v_i$ to the definition of the Pseudo Clifford operation $w_i = U^\dagger v_i U$ for 2^n elements of Pauli operations $\{v_i\}$. Our idea for searching the non-Clifford but Pseudo Clifford operation U is that we investigate unitary operations which are represented by a sum of several Pauli group operations $\{p_i\}$, namely, $U = \sum_i a_i p_i$ where a_i is a normalized coefficient ($\sum_i |a_i|^2 = 1$) and the set $\{p_i\}$ should be carefully chosen such that the sum represent a unitary operations. In this section, we present

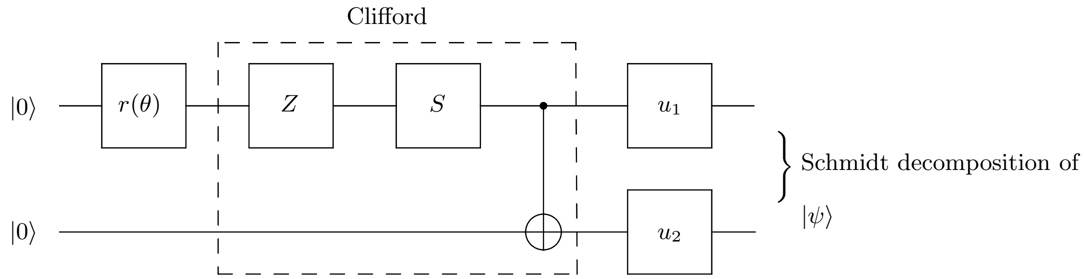

FIG. 3: A quantum circuit representing the Schmidt decomposition of two qubit state $|\psi\rangle = \cos(\theta/2)\,|a_0\rangle \otimes |b_0\rangle + \sin(\theta/2)\,|a_1\rangle \otimes |b_1\rangle$.

constructions of the local encoders for a class of states called *symmetric basis states* by finding the sum representations of the Pseudo Clifford operation generating the states. A general investigation is given in Section 4.

We first introduce symmetric basis states. Symmetric states are the states which are invariant under exchange of arbitrary two qubits. Symmetric basis states are special symmetric states. We define a n-qubit symmetric basis state $|n,m\rangle$ as a symmetric state consisting of $n-m$ qubits in $|0\rangle$ states and m qubits in $|1\rangle$ states, namely,

$$|n,m\rangle := \sqrt{\frac{m!(n-m)!}{n!}} \sum_{\pi} \pi \left(|0\rangle \otimes ... \otimes |0\rangle \otimes \overbrace{|1\rangle \otimes ... \otimes |1\rangle}^{m} \right), \tag{10}$$

where $\sum_\pi$ is taken by all permutations π of the tensor products of $(n-m)$ $|0\rangle$ states and m $|1\rangle$ states. A set of symmetric basis states of $\{|n,m\rangle\}_{m=0}^{n}$ forms a complete basis of the $(n+1)$-dimensional symmetric subspace of the n-qubit Hilbert space $\mathcal{H}^{\otimes n}$.

We consider the representation of $|n,m\rangle = U\,|\bar{0}\rangle$ using a non-local unitary operation U. The unitary operation U cannot be Pauli operations and Clifford operations for the case of $n>2$ or the case of product states $m \neq 0$ or $m \neq n$. It requires non-Clifford unitary operators to generate $|n,m\rangle$ from $|\bar{0}\rangle$, since the coefficient of the symmetric basis state $\sqrt{m!(n-m)!/n!}$ cannot be obtained by the Clifford group operations if they are not given by $1/\sqrt{2^k}$, where $k = 0,1,...,n$. In this section, we show that this U represented by a sum of Pauli group operators becomes the Pseudo Clifford operation for $|n,1\rangle$ and $|n,n-1\rangle$ symmetric basis states by choosing the appropriate local encoder and the Pauli group operations in the sum representation of U. We extend this method to show that some other symmetric basis states and related states are also locally encodable.

We first show how to represent U in the Pauli sum representation for 3-qubit symmetric basis states $|3,1\rangle$, which is alternatively called a *W state*. We consider the following set of Pauli operations:

$$\begin{aligned} \{v_0 = I \otimes I \otimes I,\ v_1 = X \otimes I \otimes I,\ v_2 = Z \otimes X \otimes I,\ v_3 = Z \otimes Z \otimes X, \\ v_4 = v_1 v_2,\ v_5 = v_2 v_3,\ v_6 = v_3 v_1,\ v_7 = v_1 v_2 v_3\} \end{aligned} \tag{11}$$

Since v_1, v_2 and v_3 forms generators $\{g_i\}_{i=1}^{3}$ of the above set $\{v_j\}_{i=0}^{7}$, we denote the set of operators generated by the generators by $\langle\{g_i\}\rangle = \langle\{v_1,\ v_2,\ v_3\}\rangle$. It is easy to check that the set $\{v_i\}$ are also local encoders for $|3,0\rangle = |\bar{0}\rangle$ and $|3,3\rangle = X \otimes X \otimes X\,|\bar{0}\rangle$.

We choose the unitary operation U_W generating the symmetric basis state $|3,1\rangle = U_W\,|\bar{0}\rangle$ in the Pauli sum representation as

$$U_W = \frac{1}{\sqrt{3}}(p_0 + p_1 + p_2) = \frac{1}{\sqrt{3}}(X \otimes Z \otimes Z + I \otimes X \otimes Z + I \otimes I \otimes X). \tag{12}$$

Note that U_W is carefully chosen such that the operators $\{p_i\}$ in the Pauli sum representation anti-commute each other to ensure the unitarity of U_W and U_W commutes with v_i. Therefore,we have

$$\langle 3,1|\, v_i^\dagger v_j\, |3,1\rangle = \langle\bar{0}|\, U_W^\dagger v_i^\dagger v_j U_W\, |\bar{0}\rangle = \langle\bar{0}|\, v_i^\dagger v_j\, |\bar{0}\rangle = \delta_{ij}, \tag{13}$$

and the set of operators $\{v_i\}_{i=0}^{7}$ given by Eq. (11) are the local encoder for $|3,1\rangle$. Since $|3,2\rangle = U_W \cdot X \otimes X \otimes X\,|\bar{0}\rangle$ and X operations applied before U_W do not change the local encoder due to Theorem II.1, $|3,2\rangle$ can be also locally encodable by the same $\{v_i\}_{i=0}^{7}$.

By generalizing the construction of the 3-qubit symmetric basis states, we show that the n-qubit symmetric basis states $|n,0\rangle$, $|n,1\rangle$ (n-qubit W state) $|n,n-1\rangle$ and $|n,n\rangle$ are also locally encodable.

Theorem III.1 ***Constructive method***
Symmetric basis states $|n,0\rangle$, $|n,1\rangle$, $|n,n-1\rangle$ and $|n,n\rangle$ are locally encodable by the Pauli operators given by

$$\langle\{g_i = Z^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}\}_{i=1}^{n}\rangle. \tag{14}$$

Proof III.1 *The product state cases ($|n,0\rangle$ and $|n,n\rangle$) are trivial. We show the proof for the case of $|n,1\rangle$. Defining a unitary operation in the Pauli sum representation*

$$U_{n,1} = \frac{1}{\sqrt{n}}\sum_{i=1}^{n} I^{\otimes(i-1)} \otimes X \otimes Z^{\otimes(i-1)}, \tag{15}$$

the symmetric basis state $|n,1\rangle$ is represented by $|n,1\rangle = U_{n,1}\,|\bar{0}\rangle$. This $U_{n,1}$ satisfies a commutation relation $[U_{n,1}, v_i] = 0$ for all i. From the relationship

$$\langle n,1|\, v_i^{\dagger} v_j\, |n,1\rangle = \langle\bar{0}|\, U_{n,1}^{\dagger} v_i^{\dagger} v_j U_{n,1}\, |\bar{0}\rangle = \langle\bar{0}|\, v_i^{\dagger} v_j\, |\bar{0}\rangle = \delta_{ij}, \tag{16}$$

the set $\langle\{g_i = Z^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}\}\rangle_{i=1}^{n}$ are the local encoder of $|n,1\rangle$. For $|n,n-1\rangle$, it is also locally encodable by the same local encoder of $|n,1\rangle$, due to the relationship $|n,n-1\rangle = U_{n,1} \cdot X \otimes X \otimes X\,|\bar{0}\rangle$ and Theorem II.1.

We can extend the locally encodable states beyond $|n,1\rangle$ and $|n,n-1\rangle$ states using the constructive method above. By replacing $U_{n,1}$ by $U_{n,1}^{\Xi} = \sum_{i=1}^{n} a_\pi I^{\otimes(i-1)} \otimes X \otimes Z^{\otimes(n-i)}$, ($a_\pi \in \mathbf{R}$) where $\sum_\pi a_\pi^2 = 1$, a state with non-even real weights on permutations can be written in the Pauli sum representation $|\Xi_{n,1}\rangle = U_{n,1}^{\Xi}\,|\bar{0}\rangle$. The state $|\Xi_{n,1}\rangle$ is also locally encodable by the local encoders of $|n,1\rangle$, since our construction does not depend on the coefficient a_π.

Next, we try to find the local encoders of other symmetric basis states by using induction.

Lemma III.1 ***Inductive method***
If $|n,k\rangle$ and $|n,k-1\rangle$ are locally encodable by the same local encoder $\{v_i\}_{i=1}^{2^n}$, then $|n+1,k\rangle$ is locally encodable by a new local encoder given by $\{I \otimes v_i, Z \otimes v_i\}$.

Proof III.2 *Since we have $|n,m\rangle = \frac{1}{2}(|0\rangle|n-1,m\rangle + |1\rangle|n-1,m-1\rangle)$, we see that*

$$\begin{aligned}\langle n+1,k|\, Z^i \otimes v_j^{\dagger} I \otimes v_k\, |n+1,k\rangle &= \frac{1}{2}\big(\langle 0|\, Z^i\, |0\rangle \langle n,k|\, v_j^{\dagger} v_k\, |n,k\rangle + \langle 1|\, Z^i\, |1\rangle \langle n,k-1|\, v_j^{\dagger} v_k\, |n,k-1\rangle\big) \\ &= \delta_{0i}\delta_{jk}.\end{aligned} \tag{17}$$

Hence, two states encoded by any two different encoding operators taken from the set $\{I \otimes v_i, Z \otimes v_i\}_{i=1}^{2^n}$ are orthogonal. Thus, $|n+1,k\rangle$ is locally encoded by $\{I \otimes v_i, Z \otimes v_i\}$.

All the 3-qubit symmetric basis states can be locally encoded by the same local encoders given by Eq. (11), we can see that the symmetric basis states of $|4,1\rangle$, $|4,2\rangle$, $|4,3\rangle$, $|5,2\rangle$, $|5,3\rangle$ and $|6,3\rangle$ are locally encodable from this lemma of the inductive method. For $|4,2\rangle$, we find that there is another local encoder given by

$$\begin{aligned}\{I \otimes v_0, I \otimes v_1, Z \otimes v_2, I \otimes v_3, Z \otimes v_4, Z \otimes v_5, I \otimes v_6, Z \otimes v_7, \\ X \otimes Z \otimes Z \otimes Z, (X \cdot Z) \otimes v_1, X \otimes v_2, (X \cdot Z) \otimes v_3, X \otimes v_4, X \otimes v_5, (X \cdot Z) v_6, X \otimes v_7\}.\end{aligned} \tag{18}$$

Due to the decomposition of $|4,2\rangle$ into $|4,2\rangle = |0\rangle \otimes |3,2\rangle/\sqrt{2} + |1\rangle \otimes |3,1\rangle/\sqrt{2}$, and using the relations of

$$\begin{aligned}\langle 3,1|\, v_1\, |3,2\rangle = -2, \langle 3,2|\, v_1\, |3,1\rangle = -2, \langle 3,1|\, v_3\, |3,2\rangle = 2, \\ \langle 3,2|\, v_3\, |3,1\rangle = 2, \langle 3,1|\, v_7\, |3,2\rangle = 1, \langle 3,2|\, v_7\, |3,1\rangle = -1,\end{aligned} \tag{19}$$

we can directly check the orthogonality of the encoded quantum states given by Eq. (18). We still do not have a construction of local encoders for $|6,2\rangle$ and $|6,4\rangle$ states, thus, it is not proven that they are locally encodable or not. The summary of locally encodable symmetric basis states and their encoders are given in Fig. 4.

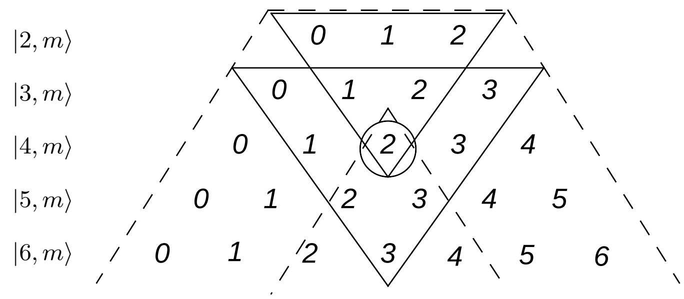

FIG. 4: Local encoding of symmetric basis states. The number m represents the number of $|1\rangle$ state. The states inside the dashed line encoded by the construction method by $\langle v_i = Z^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)} \rangle_{i=1}^n$, the states in inside the triangle line is encoded by the inductive method by $\{I \otimes v_i, Z \otimes v_i\}$. The state inside the circle is encoded by the local encoder given by Eq. (18)

IV. THE PSEUDO CLIFFORD SET AND PAULI ENCODABLE STATES

In the previous section, we have shown a constructive method for finding the local encoder set $\{v_i\}$ of symmetric basis states represented by $U|\bar{0}\rangle$ where a stronger condition $w_i = v_i$ for $U^\dagger v_i U = w_i$ is satisfied. However, in general, we can have $\{w_i\} \neq \{v_i\}$ (as we have for the more general cases in Theorem II.1). Finding the Pauli sum representation of a Pseudo Clifford operation $U = \sum_i a_i p_i$ compatible with the local encoder $\{v_i\}$ for the general cases is not straightforward. In this section, we consider a reverse engineering of this problem and present a way to derive a class of locally encodable states for a given Pauli group local encoder $\{v_i\}$ by a group theoretical analysis.

We first investigate general group theoretical properties of a unitary operator U satisfying $U^\dagger \sigma U = \sigma$ where σ is an element of the subset of the Pauli group operations and derive a formal definition of the Pseudo Clifford set. We start with defining a general subset of unitary operations.

Definition IV.1 *For a subset $\mathcal{S}$ of the Pauli group $\mathcal{P}$, a set $\mathcal{SU_S}$ of n-qubit unitary operations is defined by*

$$\mathcal{SU_S} := \{U \in SU(2^n) \mid UsU^\dagger \subset \mathcal{P}, s \in \mathcal{S}\}. \tag{20}$$

In this definition, the cardinal number of $\mathcal{S}$ is not necessarily to 2^n, but some other number m. Therefore, if we take $m < 2^n$, the set of $\mathcal{SU_S}$ implies a larger set of U than the case we have investigated for local encoding.

In Definition IV.1, we have defined that $\mathcal{S}$ is a subset of the Pauli group, however, we can extend $\mathcal{S}$ as a subgroup of the Pauli group, since for arbitrary $s_1, s_2 \in \mathcal{S}$, $Us_1s_2U^\dagger = Us_1U^\dagger Us_2U^\dagger \in \mathcal{P}$. Thus, we can choose $\mathcal{S}$ as a subgroup of the Pauli group $\mathcal{P}$. Further, we can prove that the cardinal number of $\mathcal{S}$ equals to that of $UsU^\dagger$ as in the following lemma:

Lemma IV.1 *A map $f : s \in \mathcal{S} \mapsto UsU^\dagger \in \mathcal{S}' \subset SU(2)^{\otimes n}$ is a group isomorphic mapping.*

Proof IV.1 *From the definition, the map f is surjective and homomorphism. For arbitrary $u_1, u_2 \in \mathcal{S}'$, there exist $s_1, s_2 \in \mathcal{S}$ such that $u_1 = Us_1U^\dagger, u_2 = Us_2U^\dagger$ since the map f is surjective. Then, $s_1 = s_2$ if $u_1 = u_2$.*

From Lemma IV.1, we give a formal definition of the Pseudo Clifford set.

Definition IV.2 ***(Pseudo Clifford set)***
For subgroups P_1 and P_2 ($|P_1| = |P_2|$) of the Pauli group P, the corresponding Pseudo Clifford set $\mathcal{C}(P_1, P_2)$ is defined by

$$\mathcal{C}(P_1, P_2) := \{U \in SU(2^n) \mid UP_1U^\dagger = P_2,\ P_1, P_2 \subset \mathcal{P}\}. \tag{21}$$

Hence Pseudo Clifford sets are defined with respect to particular Pauli subgroups P_1 and P_2 - and they conjugate one to the other. The set $\mathcal{C}(P_1, P_2)$ equals to the Clifford group $\mathcal{C}$ if $P_1 = P_2 = \mathcal{P}$ and is not necessarily a group.

For local encoding, we require $|P_i| = 2^n$. We would have P_1 in Definition 21 is given by $\langle \{g_i\}_{i=1}^n \rangle$, where $\{g_i\}_{i=1}^n$ are generators of the Pauli local encoder set $\{v_i\}$. We take $g_i = v_i$ for $i = 1, ..., n$. Since a Pseudo Clifford operator U satisfies

$$\langle \bar{0}| U^\dagger v_i^\dagger v_j U |\bar{0}\rangle = \langle \bar{0}| w_i^\dagger U^\dagger U w_j |\bar{0}\rangle = \langle \bar{0}| w_i^\dagger w_j |\bar{0}\rangle = \delta_{ij} \tag{22}$$

for arbitrary $v_i, v_j \in P_2$, a state given by $U|\bar{0}\rangle$ is locally encodable. We call a state represented by U as the *Pauli encodable state*. Our goal in this section is to derive a set of Pauli encodable states for a given Pauli local encoder $\{v_i\} \in \mathcal{C}(P_1, P_2)$.

By denoting a generator of the local encoder $\{w_i = Uv_iU^\dagger\} \in P_2$ of $|\bar{0}\rangle$ by $\{g'_i\}_{i=1}^n$, we reduce the relationship for the local encoders $\{v_i\}$ and $\{w_i\}$ to the relationship for the generators $\{g_i\}$ and $\{g'_i\}$. Further, since Clifford operations give a way to map a generating set of Pauli operations to another generating set, there always exists a Clifford operation C such that

$$C^\dagger U g_i U^\dagger C = C^\dagger g'_i C = g_i, \rightarrow W g_i V^\dagger = g_i \tag{23}$$

for an arbitrary g_i, where $W = C^\dagger U$. Therefore, we can assume that W maps all the elements of P_1 to themselves. This result shows that multiplication of appropriate Clifford operation $C^\dagger$ reduces our problem to a simple case of $g'_i = g_i$, which we have investigated in Section 3.

To obtain the non-Clifford but Pseudo Clifford operation W, we define an hermitian commutative set $\mathcal{L}$ by

$$\mathcal{L} = \{p \in \mathcal{P} \mid [p, g_i] = 0,\ p : \text{Hermitian},\ \forall g_i \in \{g_i\}_{i=1}^n\}. \tag{24}$$

Thus, we can construct a subgroup $\mathcal{SU}_\mathcal{L}$ of $SU(2^n)$, because $\mathcal{L}$ is a subalgebra of the Lie algebra of $SU(2^n)$. From the definition of $\mathcal{L}$, all the elements of $\mathcal{SU}_\mathcal{L}$ commute with all the elements of $\mathcal{S}$. Therefore, we obtain a Pauli encodable state represented by $CW|\bar{0}\rangle\, (C \in \mathcal{C},\ W \in \mathcal{SU}_\mathcal{L})$.

Our method for obtaining the Pauli encoders is summarized in the following steps.

1. Choose a set of Pauli generator $\{g_i\}_{i=1}^n$ for the zero state $|\bar{0}\rangle$.
2. Construct a hermitian commutative set $\mathcal{L}$ defined by Eq. (24) associated with the generators $\{g_i\}_{i=1}^n$.
3. Construct a Lie group $\mathcal{SU}_\mathcal{L}$ from the Lie subalgebra $\mathcal{L}$. We call the Lie group $\mathcal{SU}_\mathcal{L}$ a Pauli encoder group.
4. For an arbitrary Clifford operation C and an arbitrary $W \in \mathcal{SU}_\mathcal{L}$, we obtain a Pauli encodable state $CW|\bar{0}\rangle$ and a Pauli encoder $\langle\{Cg_iC^\dagger\}_{i=1}^n\rangle$.

In general the difficulties arise in step ii) - not all generator sets will allow for a nice construction of $\mathcal{L}$ (24). We show two concrete constructions for the Pauli encodable states for given Pauli encoders in the followings. If the generator is given by $\{g_i = I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}\}$, we have the hermitian commutative set $\mathcal{L}$ defined by

$$\mathcal{L} = \{q_i \equiv X^{i_1} \otimes X^{i_2} \otimes \cdots \otimes X^{i_n},\ i := i_1 i_2 \cdots i_n \in \mathbb{Z}_2^n\}. \tag{25}$$

Thus, an element $W \in SU_L$ is given by

$$W = \exp[i \sum_{i \in \mathbb{Z}_2^n} c_i q_i],\ (c_i \in \mathbb{C}). \tag{26}$$

Therefore, with an arbitrary Clifford operation C, a Pauli encodable state is given by

$$C \exp[i \sum_{i \in \mathbb{Z}_2^n} c_i q_i]\, |\bar{0}\rangle\,, \tag{27}$$

and the corresponding Pauli encoder is given by

$$\langle\{C \cdot (I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)})) \cdot C^\dagger\}_{i=1}^n\rangle. \tag{28}$$

If the generator is given by $\{g_i = Z^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}\}_{i=1}^n$, we have the hermitian commutative set $\mathcal{L}$ defined by

$$\mathcal{L} = \langle\{q'_i \equiv I^{\otimes(i-1)} \otimes X \otimes Z^{\otimes(n-i)}\}_{i=1}^n\rangle. \tag{29}$$

Thus, with an arbitrary Clifford operation C, a Pauli encodable state is given by

$$C \exp[i \sum_{i=0}^n c_i q'_i]\, |\bar{0}\rangle\,, \tag{30}$$

where we take $p'_0 = I^{\otimes n}$. The corresponding Pauli encoder is given by

$$\langle\{C \cdot (Z^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}) \cdot C^\dagger\}_{i=1}^n\rangle. \tag{31}$$

We see that the symmetric basis state $U_{n,1}$ is a special case of Eq. (30).

V. CONCLUSION AND DISCUSSION

In this work we have looked at the possibility of encoding classical information onto quantum states by local unitary operations. We have presented explicit encodings for large sets of states including all stabiliser and various symmetric basis states. We have introduced the notion of Pseudo Clifford which unifies these states under one general local encoding method. Finally, by resorting to group theoretic analysis we have given a method to find large sets of states with the same local encodings.

Although the methods used for local encoding presented here are not as general as possible, we have not been able to show that there are any states which cannot be encoded by our methods, and it remains an open problem wether all states can be locally encoded by Pauli operations, or indeed at all.

We may also be interested in different ways of local encoding for other reasons and applications. For example in dense coding [4, 10] we wish to encode the information by acting on only a subset of the parties (the idea being that then by sending that same subset through a quantum channel, we can communicate more information than the that allowed by the Holevo bound). The local encoding presented here could not be used for such a protocol. We can then ask can we extend these results to consider such protocols, or what can our results say about when we can or cannot.

For example, we know that for optimum dense coding, we must have a maximally entangled state between the senders and receivers. Imagine we try to dense code using the state $|\psi\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{i=0}^{2^{n-1}} U|i\rangle_s \otimes |i\rangle_r \in \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$, where $|i\rangle_x$ are the product states of the computational basis over the senders' and receivers' spaces for subscripts s and r respectively. The Schmidt basis on the side of the senders (subscript s) is in general entangled across the set of senders by unitary U. If U is just identity, then we can encode simply using the Pauli operators [10]. Surprisingly we can see that the senders can still encode the full basis locally, independent of U. This can be easily, since for optimal dense coding, we would require $\langle\psi|\, v_i^\dagger \otimes \mathbb{1} \cdot v_j \otimes \mathbb{1}\, |\psi\rangle = \delta_{ij}$ for all i, j. It is easy to see that the U drops out and the condition is equivalent to simply $Tr[v_i^\dagger v_j] = 0$. This is satisfied for the local Pauli, hence they allow dense coding for these states. Thus maximum entangled states can be always optimally locally dense coded independent of the Schmidt basis. The same result can be obtained by using the Choi-Jamiolkowski isomorphism [11] by bringing the unitary over to the receiver's side $|\psi\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{i=0}^{2^{n-1}} U|i\rangle_s \otimes V|i\rangle_r = \frac{1}{\sqrt{2^{n-1}}} \sum_{i=0}^{2^{n-1}} |i\rangle_s \otimes U^T V|i\rangle_r$. In this way it is clear that the standard Pauli approach will work from [10].

We can also note that some of the states considered here have mirror results in local decoding. It is known that the ability to decode such encoded classical information is bounded by the entanglement[12], and explicit bounds are given for W-states and large sets of graph states (which, in the case of graph states can be made tight [13]). We can thus compare the amount of information we can encode to that we can decode $\Delta I_{local} = I_{local\ encodable} - I_{local\ decodable}$. For graph states this gives $\Delta I_{local} = E(|\psi\rangle) = n/2$. Indeed, from [13] for all states where we can locally encode we have $\Delta I_{local} \geq E(|\psi\rangle)$. This allows us to talk about a kind of irreversibility of local information - we can encode much easier than decode locally, and the difference is bounded by the entanglement. It is interesting to consider what such a quantity would mean in relation to other tasks such as measurement based quantum computing, error correction e.t.c.

We see then that there are many open questions remaining, and that these results may have potential interest in various areas of quantum information processing and studies of locality. In addition we may also consider the usefulness of the task directly in many-party quantum cryptographic scenarios where we have distributed encoders and decoders. These will be the topics of ongoing study.

Acknowledgements

We are very grateful to Akimasa Miyake, Shashank Virmani, Masaki Owari, Toshio Ohshima and Terry Rudolph for stimulating discussions on this topic. This work was sponsored by the Asahi Glass Foundation and the Japan Society for the Promotion of Science.

[1] C. H. Bennett and G. Brassard. 1984. in Proc. IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984).
[2] A. Ekert. *Phys. Rev. Lett.*, 67(661), 1991.
[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. *Phys. Rev. Lett*, 70(1895), 1993.
[4] C. H. Bennett and S. Weisner. *Phys. Rev. Lett*, 69(2881), 1992.
[5] R. Raussendorf and H. J. Briegel. *Phys. Rev. Lett.*, 86(5188), 2001.

[6] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. *Phys. Rev. A*, 59(1070), 1999.

[7] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. *Phys. Rev. Lett.*, 82(5385), 1999.

[8] M. Hein, W. Dür, J. Eisert R. Raussendorf, M. Van den Nest, and H. J. Briegel. 2005. quant-ph/0602096.

[9] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[10] D. Bruß, G. M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen. *Phys. Rev. Lett.*, 93(210501), 2004.

[11] M.-D Choi *Lin. Alg. Appl.*, 10 (285), 1975; A. Jamiolkowski *Rep. Math. Phys.*, 3 (275), 1972.

[12] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani. *Phys. Rev. Lett.*, 96(040501), 2006.

[13] D. Markham, A. Miyake, and S. Virmani. 2006. quant-ph/0609102.